In a more general application of the invention, as shown in FIG. **2**, the representation, e.g., a hash, of a particular document is simply concatenated with the catenate certificate value of the next previous document and the deterministic function representation, again a hash, for example, of this composite is then generated and retained as the record catenate value for the particular document Each subsequent document in the growing series is similarly processed to expand the record which itself would serve as a reliable certification of the position each such document occupies in the series, or more broadly viewed, in the continuum of time. This embodiment of the invention provides a reliable method by which an organization, for instance, could readily certify the sequence and continuity of its digital business documents and records.

Additional variations in the process of the invention might include the accumulation of documents, preferably in hashed or other representative form, generated within an author organization over a period of time, e.g. a day or more depending upon the extent of activity, with the collection being hashed to present a single convenient document for time-stamping and certification. As an alternative, an organizational designee might serve as a resident "outside" agency who would maintain a catenate certificate record of organization documents by means of the present procedure and on a regular basis would transmit the then current catenate certificate to a TSA. In this manner the sequence of an organization's business records would be established both within the organization and externally through the TSA.

Also, the implementation of process embodiments might readily be automated in simple computer programs which would directly carry out the various steps of hashing, transmitting, and concatenating original document representations, applying current time stamps, generating and recording catenate certificate values, and providing receipt certificates.

THE DRAWING

The present invention will be described with reference to the accompanying drawing of which:

FIG. **1** is a flow diagram of an embodiment of the time-stamping process according to the invention; and

FIG. **2** is a flow diagram of the general catenation process according to the invention.

DESCRIPTION OF THE INVENTION

The following exemplary application of the present invention, as depicted in the steps of the drawing, will serve to further describe the time-stamping process. For convenience in the presentation of this example, the deterministic function employed is the **md4** hashing algorithm described by Rivest, as mentioned above; however, the function actually selected by a TSA could be any of various available algorithms. Whatever algorithm is implemented, records of its identity and period of use must be maintained for later proof of certified receipts.

The present time-stamping procedure begins, as at step **11** of the drawing, with the preparation of a digital document by the author, e.g. A_k. As previously noted, this digital document may be the digital form or representation of any alphanumeric text or video, audio, pictorial or other form of fixed data. Although the present process may be used with documents of any length, the following excerpt is amply representative of a document, D_k, for which time-stamping is desired:

> . . . the idea in which affirmation of the world and ethics are contained side by side . . . the ethical acceptance of the world and of life, together with the ideals of civilization contained in this concept . . . truth has no special time of its own. Its hour is now—always.
>
> Schweitzer

If the author so desires, the document, D_k, may, for the purposes of security as well as to reduce the required transmission bandwidth, be condensed by means, for example, of the **md4** algorithm. As indicated by the optional, dashed step **12**, the document is thus hashed to a value, H_k, of a standard 128 bit format which, expressed in base **16**, appears as:

ee2ef3ea60df10cb621c4fb3f8dc34c7

It should be noted at this point that the hexadecimal and other numerical value representations used in this example are not in such form crucial to the implementation of the invention. That is to say, any portion or other distinct representation of those values selected according to a given procedure would function as well.

Author, A_k, whose assigned identification number, ID_k, is 634 in a 1000 member author universe, then transmits the document, at step **13**, to the system TSA in the identifying message, (ID_k, H_k), which appears:

634, ee2ef3ea60df10cb621c4fb3f8dc34c7

as a request that the document be time-stamped.

The TSA, at step **14**, prepares the receipt for document, D_k, by adding a sequential receipt transaction number, r_k, of 1328, for example, and a statement of the current time, t_k. This time statement might be a standard binary representation of computer clock time or simply a literal statement, e.g., 19:46:28 Greenwich Mean Time on Mar. 6, 1991, in order to allow the final time-stamp certificate to be easily read. The receipt then comprises the string, (r_k, t_k, ID_k, H_k), which appears as follows;

1328, 194628GMT06MAR91, 634,
ee2ef3ea60ef10cb621c4fb3f8dc34c7

In accordance with the invention, the records of the TSA at this time contain a catenation of all its prior receipt transactions in the form, for example, of the values resulting from the hashing of each consecutive receipt with the record catenation to that time. This catenate record would thus have been developed as follows. The receipt of first transaction ($r_{k=1}$) was hashed with an initial datum value, e.g., the hash of the identification of the TSA, to yield the first catenate value, C_1, which was then used as the certificate value for that first transaction. In the next transaction, the receipt was concatenated with $C_1$and the composite hashed to yield the second catenate certificate value, C_2, and so on through the entire history of the TSA time-stamping operation.

Assume now that the document, D_{k-1}, immediately preceding that of the present example had been processed by the TSA, in its 1327th receipt transaction, to yield as the catenate certificate value, C_{k-1}:

26f54eae925156b1f0d6047c2de6e0fcf

In step **15** of the process, the TSA now concatenates with this value the receipt for D_k to obtain: